Blockchain: A Disruption Technology

Part I: Bitcoin and Cryptocurrencies

Topic 4 AFIN8014 FinTech and Innovation

Learning Objectives

1 Understand what is 'Money' and its evolution

2 Understand the main issues of the fiat currency

3 Identify what is a Bitcoin and how Bitcoin might address the issues of fiat currency

4 Discuss the technology behind Bitcoin: blockchain

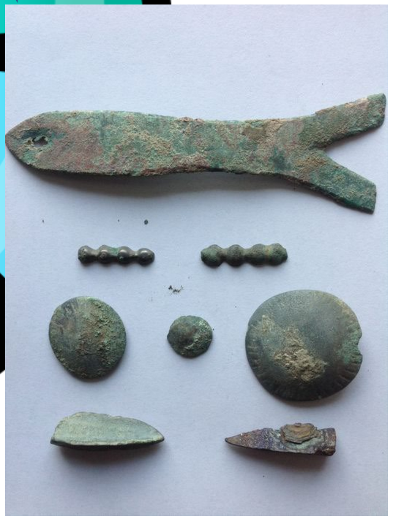
5 Get insight into cryptocurrencies and how to evaluate them

- 9000BC
- Barter goods in surplus for ones they lack
- First recorded in Egypt

Money History

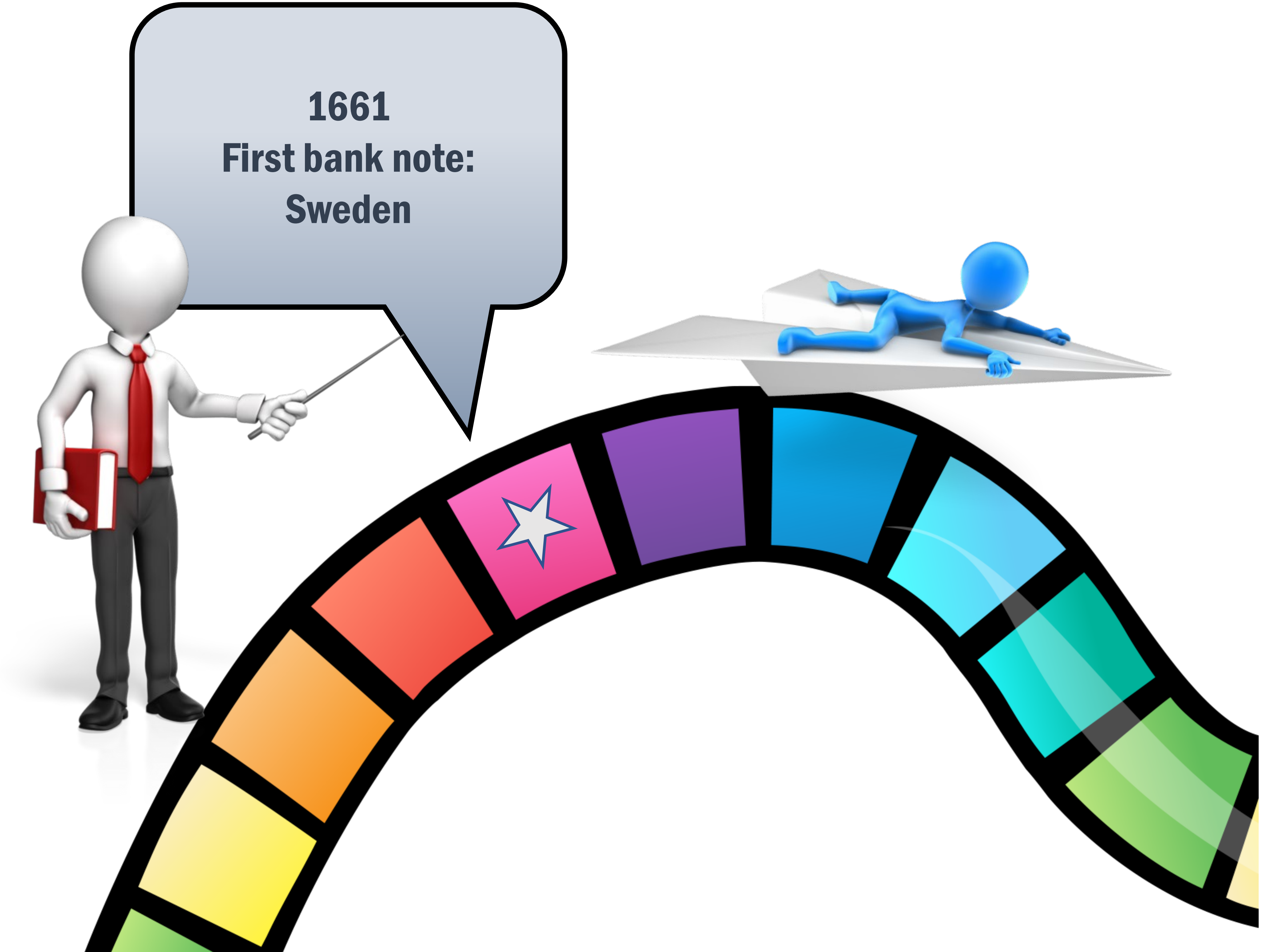
600BC
The first 'official' coin in Lydia (Turkey)

1100BC
In China, people started to using small replicas of goods cast from bronze



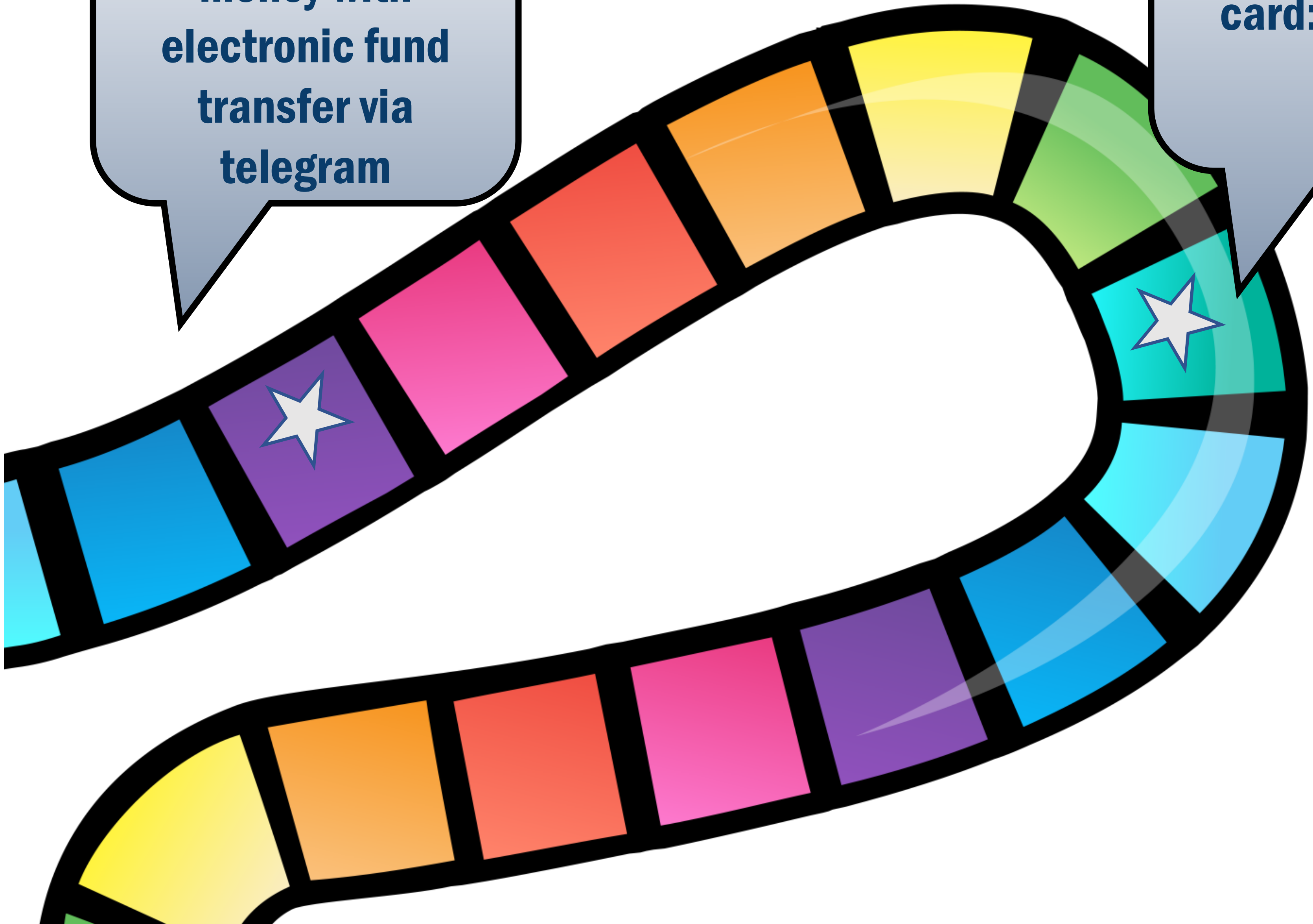
960–1279

- The first paper money: Jiaozi, Song Dynasty, China
- The travels of Marco Polo to China introduced the idea of paper money to Europeans



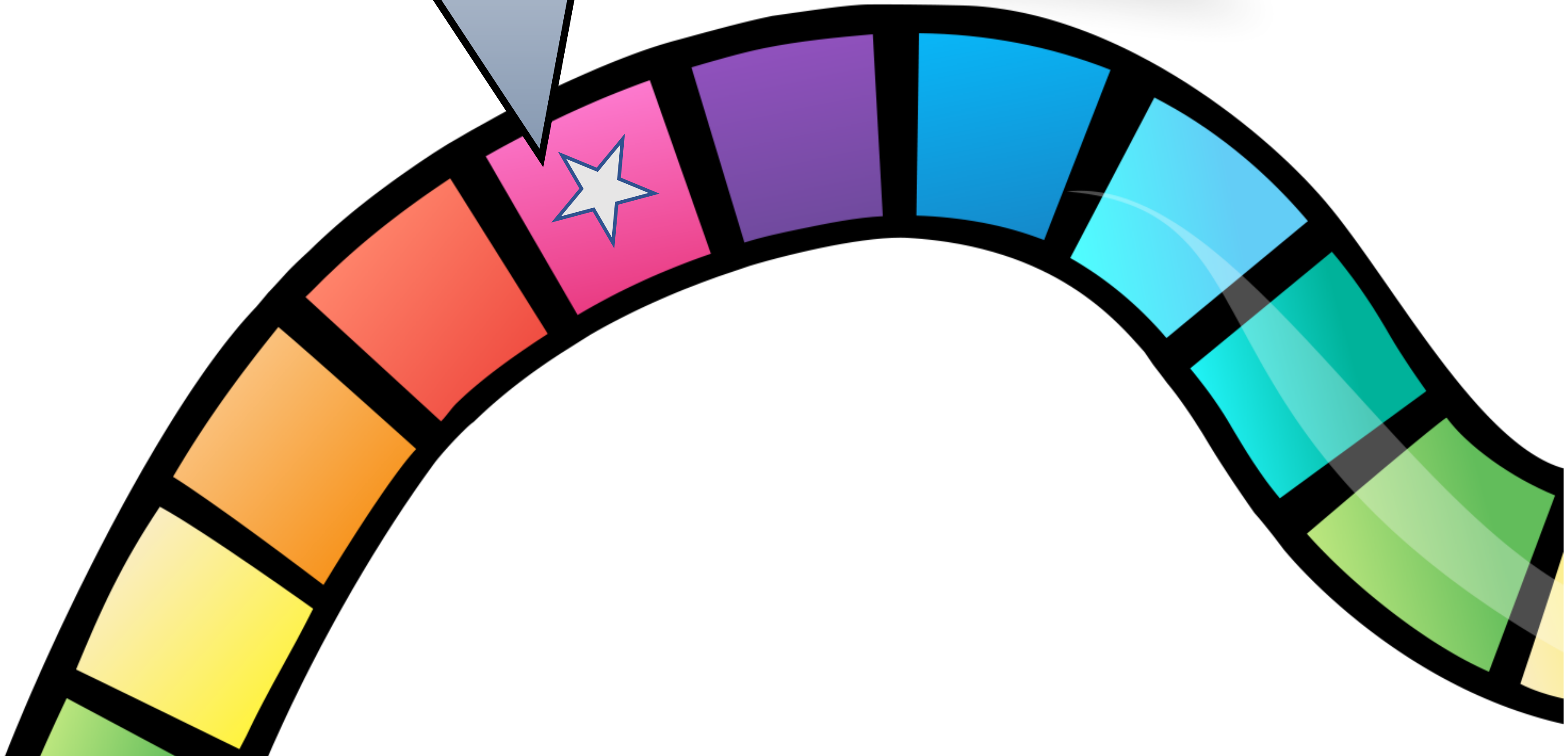
1661
First bank note:
Sweden

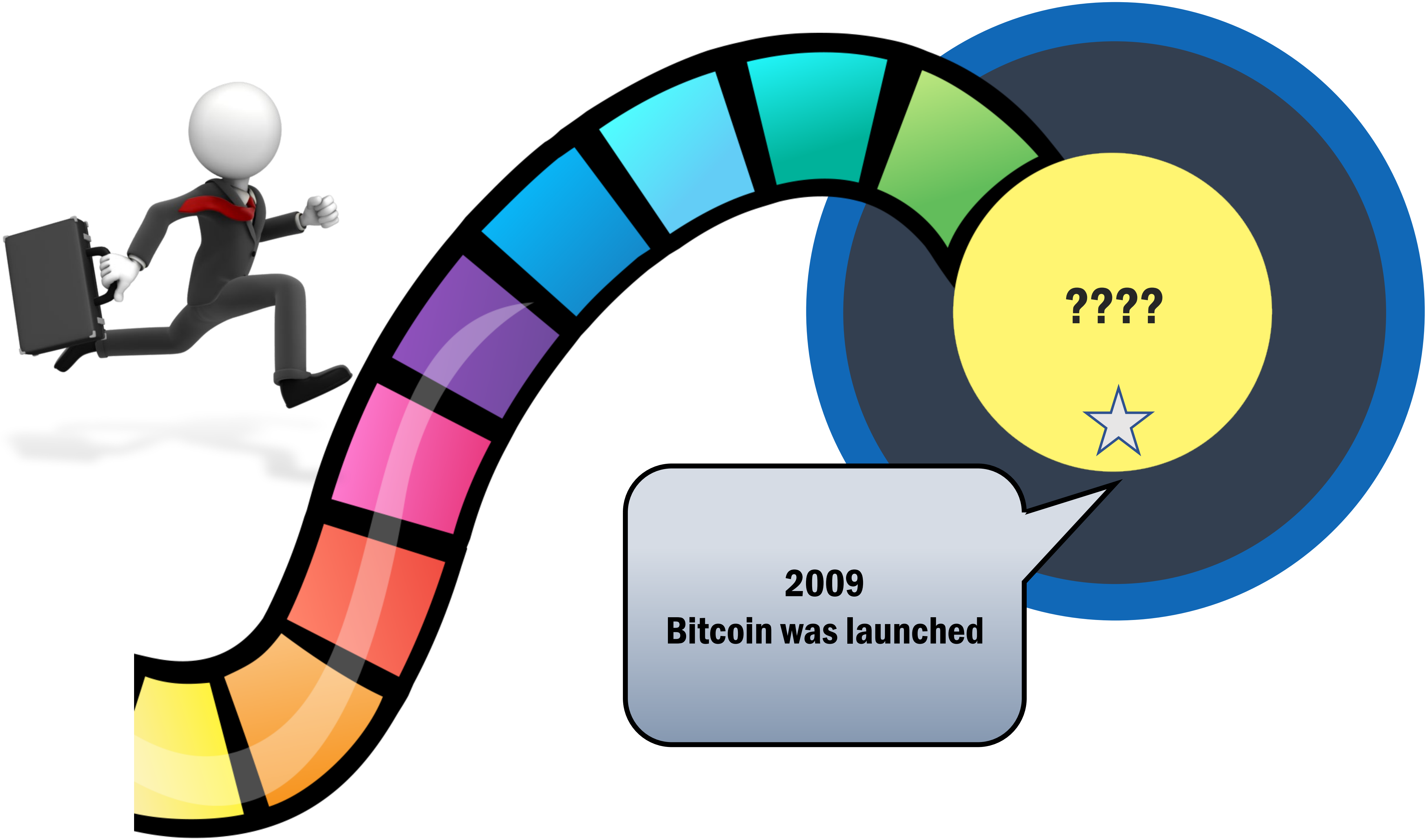
1860
Western Union, e-money with electronic fund transfer via telegram



1946
The first creditt card: ‘Charg-it’ Card

1999
European banks began offering mobile banking





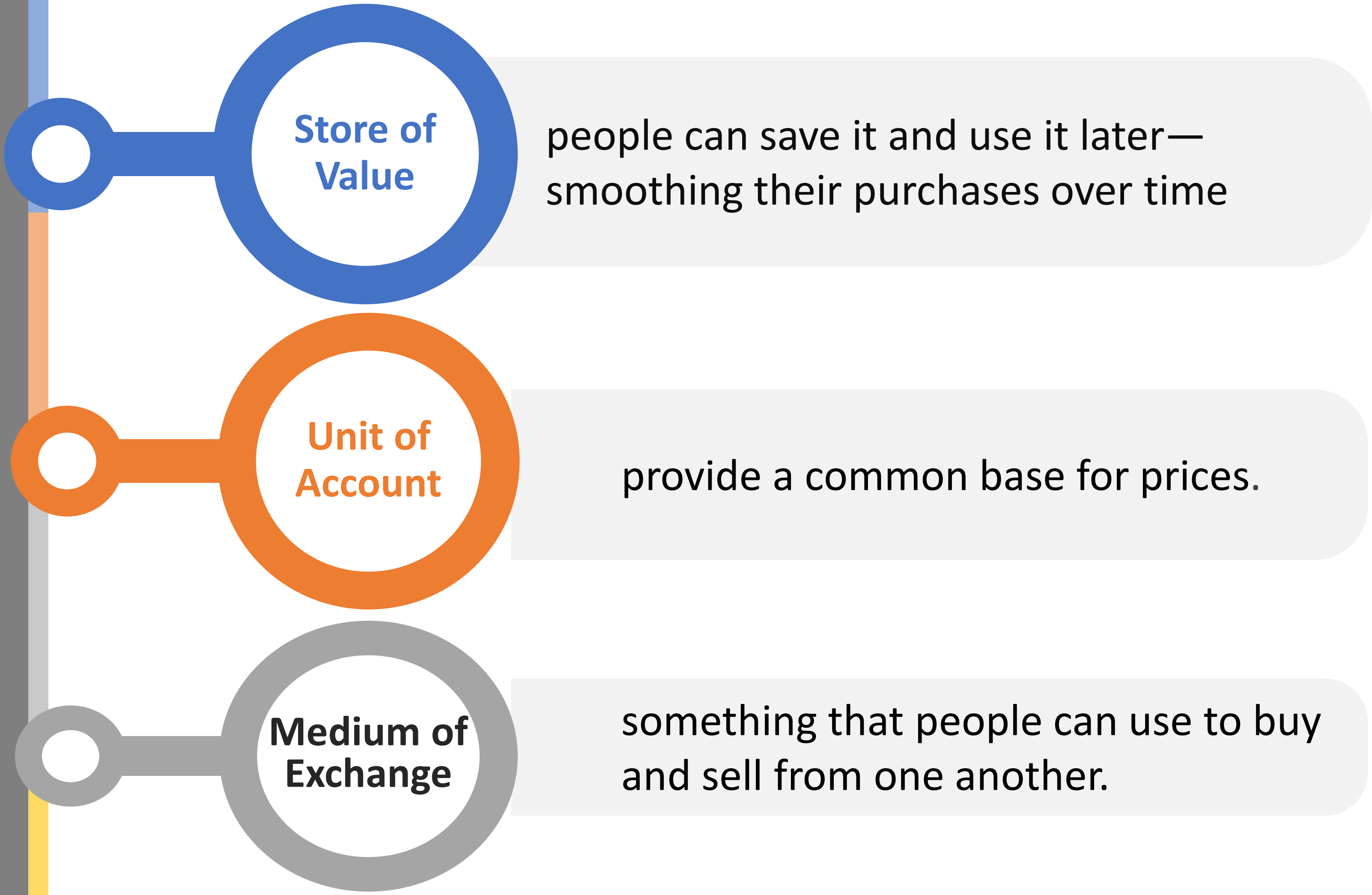
????

2009
Bitcoin was launched

What is Money?

Money evolves (forms and shapes)

Bottom-Line: the common beliefs of the individual users



Store of Value: people can save it and use it later—smoothing their purchases over time

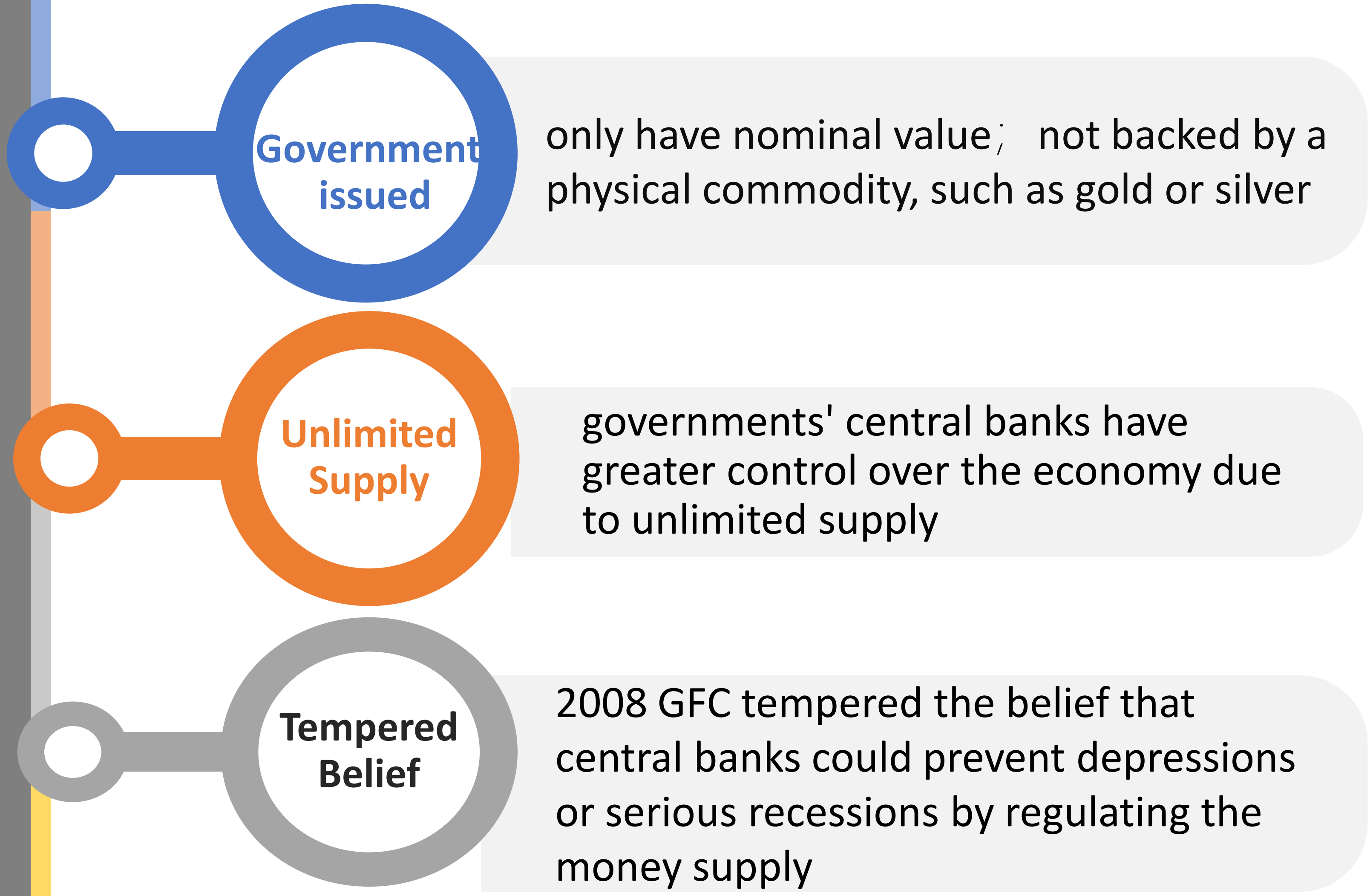
Unit of Account: provide a common base for prices.

Medium of Exchange: something that people can use to buy and sell from one another.

Today’s Money:
Fiat Money

No use value

People believes its value



Government issued

only have nominal value； not backed by a physical commodity, such as gold or silver

Unlimited Supply

governments' central banks have greater control over the economy due to unlimited supply

Tempered Belief

2008 GFC tempered the belief that central banks could prevent depressions or serious recessions by regulating the money supply

Fiat Money: Problems and Solutions?

Problems

A Possible Solution?

Centrally Controlled → Decentralized

January 2009

Unlimited Supply → Limited Supply

In October 2008, metzdowd.com

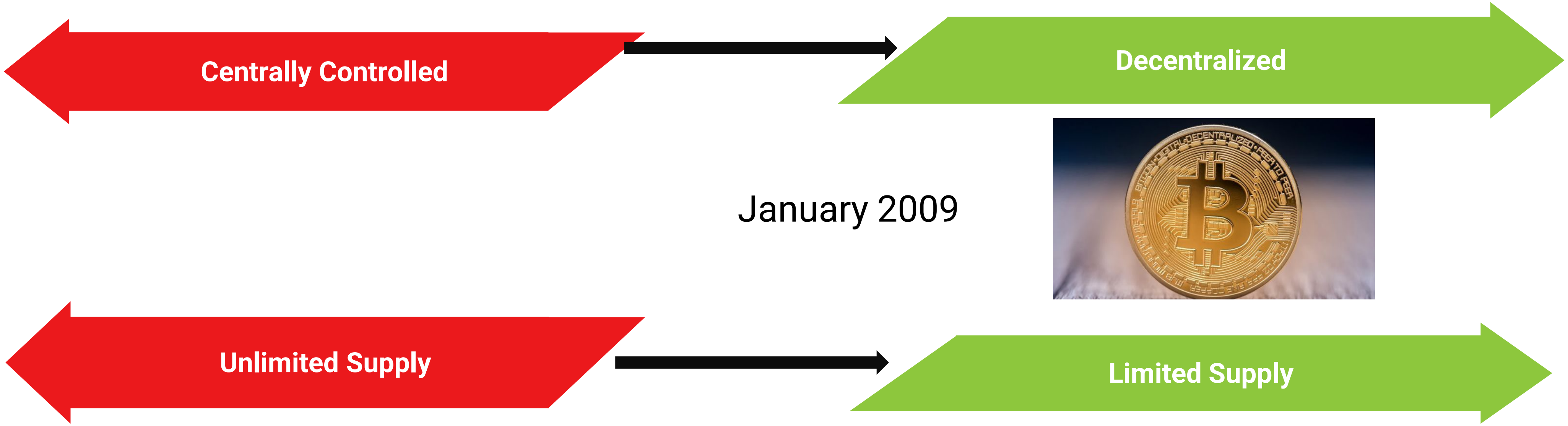
‘Bitcoin: A Peer-to-Peer Electronic Cash System’

Satoshi Nakamoto

Fiat Money: Problems and Solutions?

Problems

A Possible Solution?



Centrally Controlled

Decentralized

January 2009

Unlimited Supply

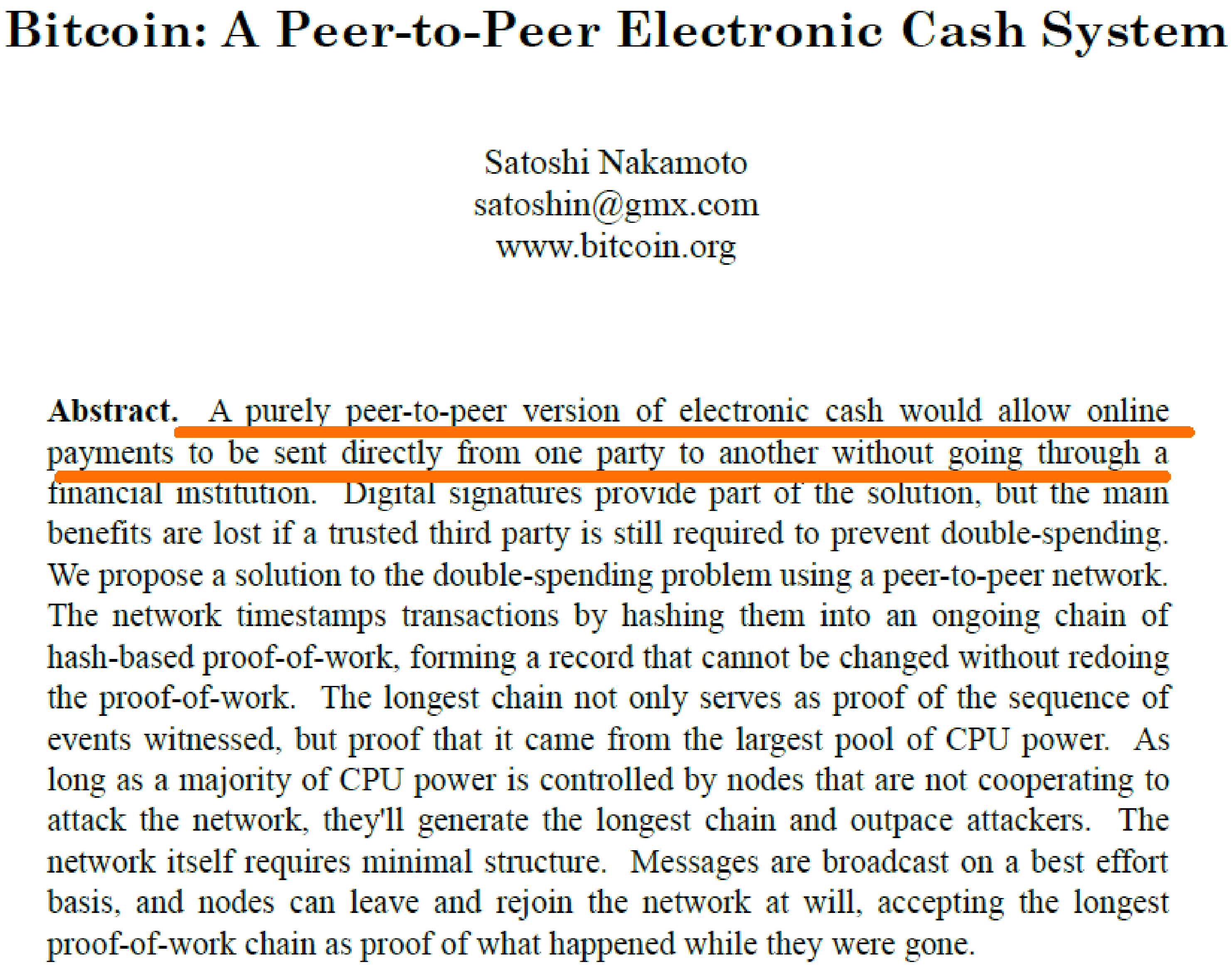
Limited Supply

In October 2008, metzdowd.com

‘Bitcoin: A Peer-to-Peer Electronic Cash System’

Satoshi Nakamoto

Bitcoin: A Peer-to-Peer Electronic Cash System



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Bitcoin

- Common beliefs
- Decentralized
- Limited Supply
- Cryptographic digits

If everyone **agrees the value** of Bitcoin, it is the money

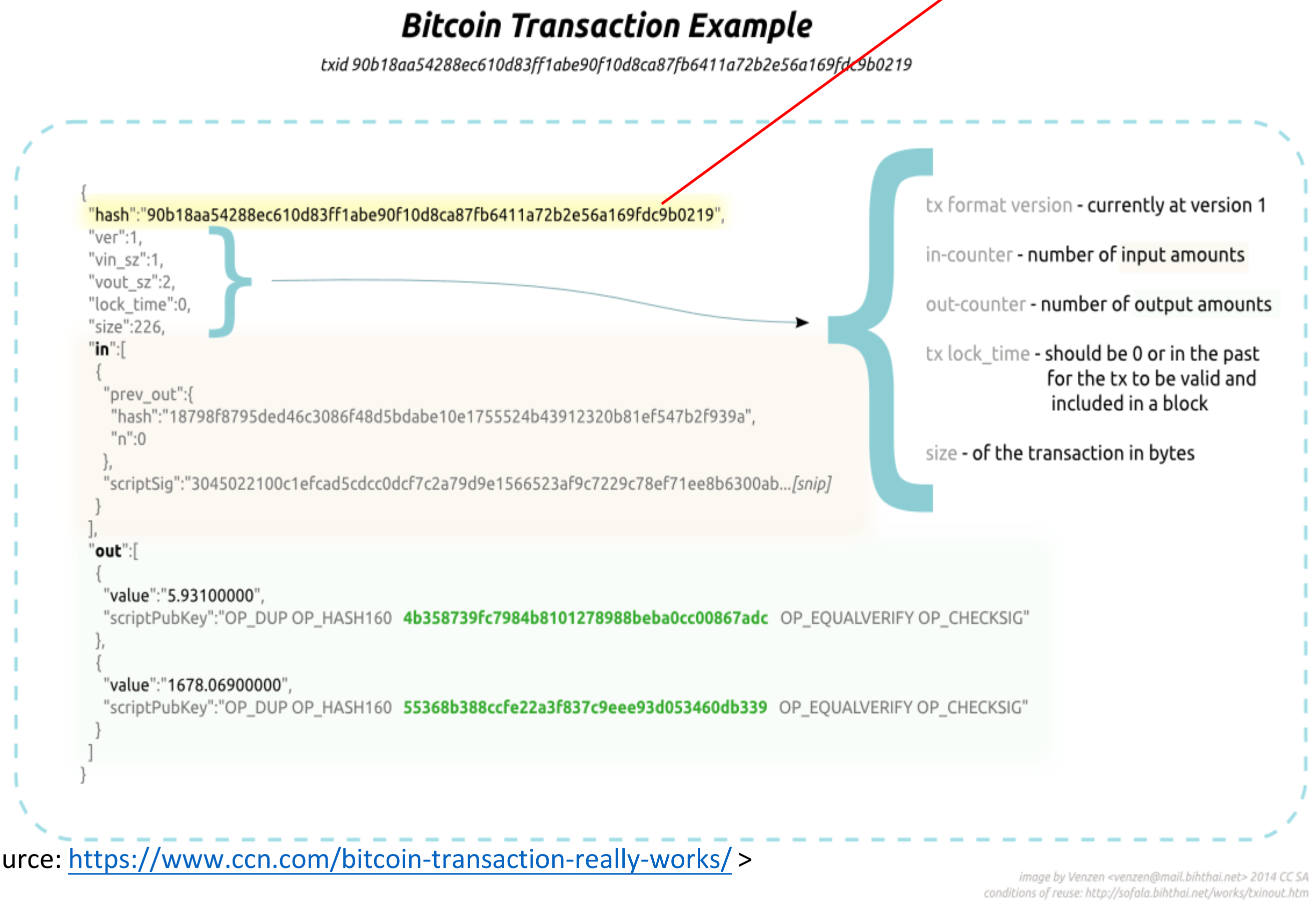
In lieu of intermediated governance, Bitcoin holders govern themselves through a publicly sharing **blockchain** ledger

A monetary policy based on artificial scarcity : total number of bitcoins could never exceed **21 million**.

cryptocurrency : a digital asset designed to work as a medium of exchange that uses strong cryptography

How Does Bitcoin Look Like?

Online and Digital



Bitcoin Transaction Example

txid 90b18aa54288ec610d83ff1abe90f10d8ca87fb6411a72b2e56a169fdc9b0219

```
{
 "hash":"90b18aa54288ec610d83ff1abe90f10d8ca87fb6411a72b2e56a169fdc9b0219",
 "ver":1,
 "vin_sz":1,
 "vout_sz":2,
 "lock_time":0,
 "size":226,
 "in":[
  {
   "prev_out":{
    "hash":"18798f8795ded46c3086f48d5bdabe10e1755524b43912320b81ef547b2f939a",
    "n":0
   },
   "scriptSig":"3045022100c1efcad5cdcc0dcf7c2a79d9e1566523af9c7229c78ef71ee8b6300ab...[snip]
  }
 ],
 "out":[
  {
   "value":"5.93100000",
   "scriptPubKey":"OP_DUP OP_HASH160  4b358739fc7984b8101278988beba0cc00867adc  OP_EQUALVERIFY OP_CHECKSIG"
  },
  {
   "value":"1678.06900000",
   "scriptPubKey":"OP_DUP OP_HASH160  55368b388ccfe22a3f837c9eee93d053460db339  OP_EQUALVERIFY OP_CHECKSIG"
  }
 ]
}
```

tx format version - currently at version 1

in-counter - number of input amounts

out-counter - number of output amounts

tx lock_time - should be 0 or in the past for the tx to be valid and included in a block

size - of the transaction in bytes

image by Venzen <venzen@mail.bihthai.net> 2014 CC SA
conditions of reuse: http://sofala.bihthai.net/works/txinout.htm

Bitcoin Transaction Example <source: https://www.ccn.com/bitcoin-transaction-really-works/ >

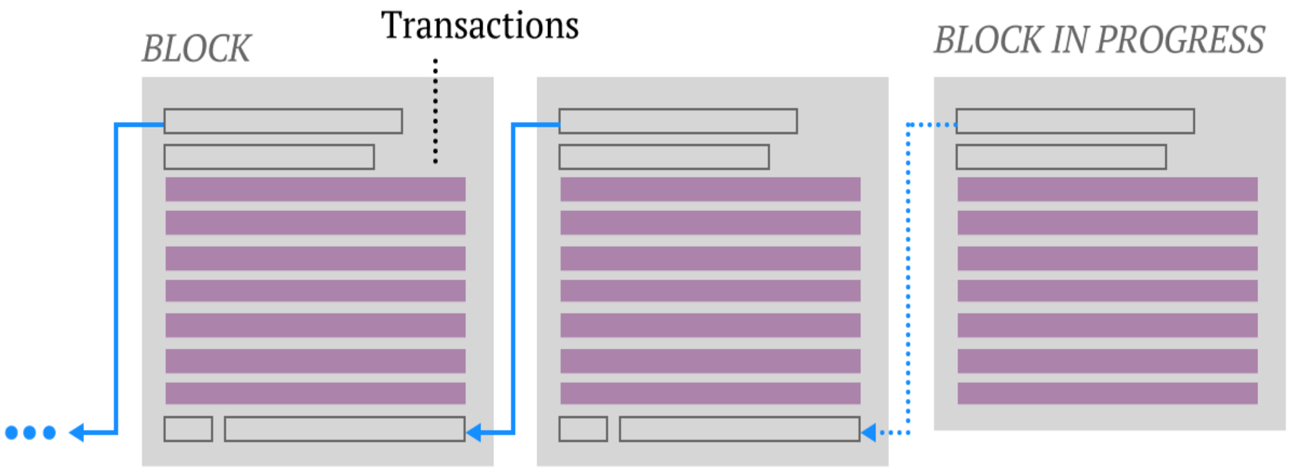
A **cryptographic hash output**

- The result of a transformation of the original information (input)
- It is a long, unique string of **numbers**
- Based on a mathematical algorithm
- SHA-256

https://www.movable-type.co.uk/scripts/sha256.html

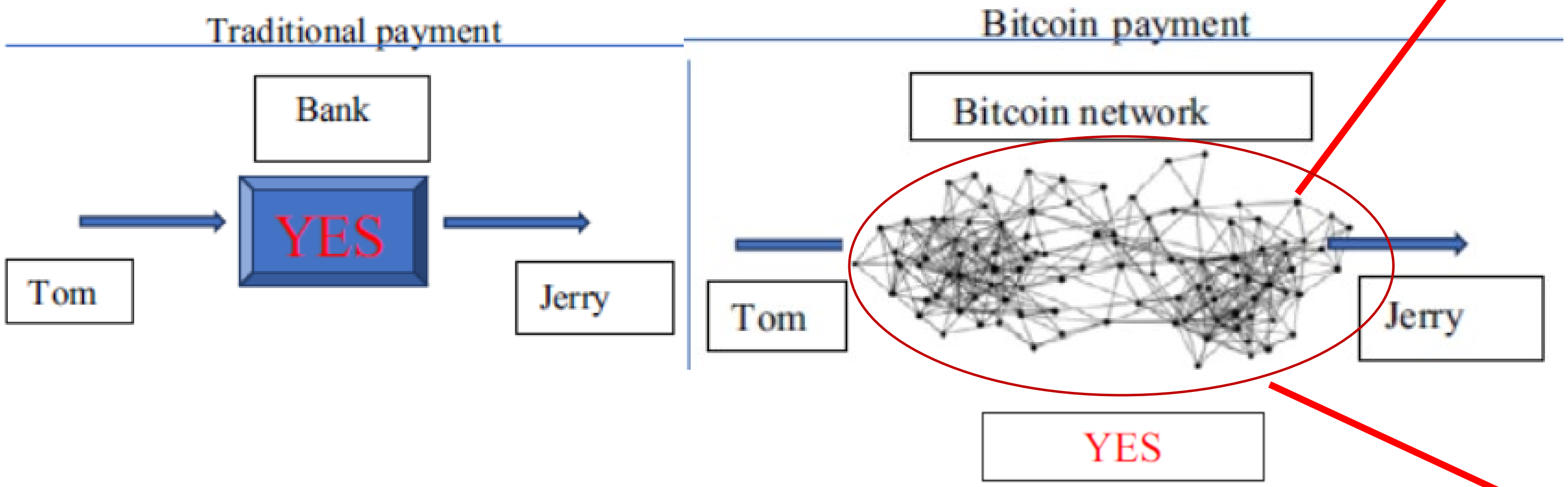
Blockchain: the Technology underlying Bitcoin

- Bitcoin: a **chian** of digital signature
- Bitcoin transaction (transfer the ownership of bitcoin): recorded in forms of **blocks**.
- Each block includes a reference to the block that came before it. This lineage of blocks is the block chains which are built with **hash pointers** (a hash pointer is where data is stored together with a cryptographic hash of the value of that data).
- Blockchain : **is a linked-list (a ledger)**



Source: Figure retrieved from https://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins/

How Does Bitcoin Work?



Node: who keeps a copy of the blockchain ledger and runs the appropriate software to approve new additions to the blockchain.

Network: The collective group of node
A Peer-to-peer **decentralized** network without a centralized authority.

Event: **Tom paid $100 to Jerry**
1. broadcast this transaction to all of the Bitcoin nodes
2. The **majority** of nodes must **agree** on the transaction.
3. Once the network accepts Tom’s transaction, this new transaction will be added into the public ledger as a new hash in a block.

Key: The agreement of decentralized nodes and the public ledger facilitates this Bitcoin transaction **verification**.

Bitcoin Innovation

- How do nodes **reach a consensus** regarding Tom’s transaction?
- How to guarantee Tom’s transaction is **truthfully** recorded?

Technical methods +Incentive Engineering

Bitcoin Miner

Satoshi’s solution

Technical

Blockchain with Cryptographic Information

- collision-resistance
- hiding
- puzzle-friendliness

Incentive

Good enough to behave honestly

- **Competing** to solve a hash puzzle to be the one to add Tom’s transaction in the public ledger.
- Be **rewarded** with Bitcoin(s) (block reward) and transaction fees.
- A proof-of-work (**PoW**) mechanism.

Main Take Away

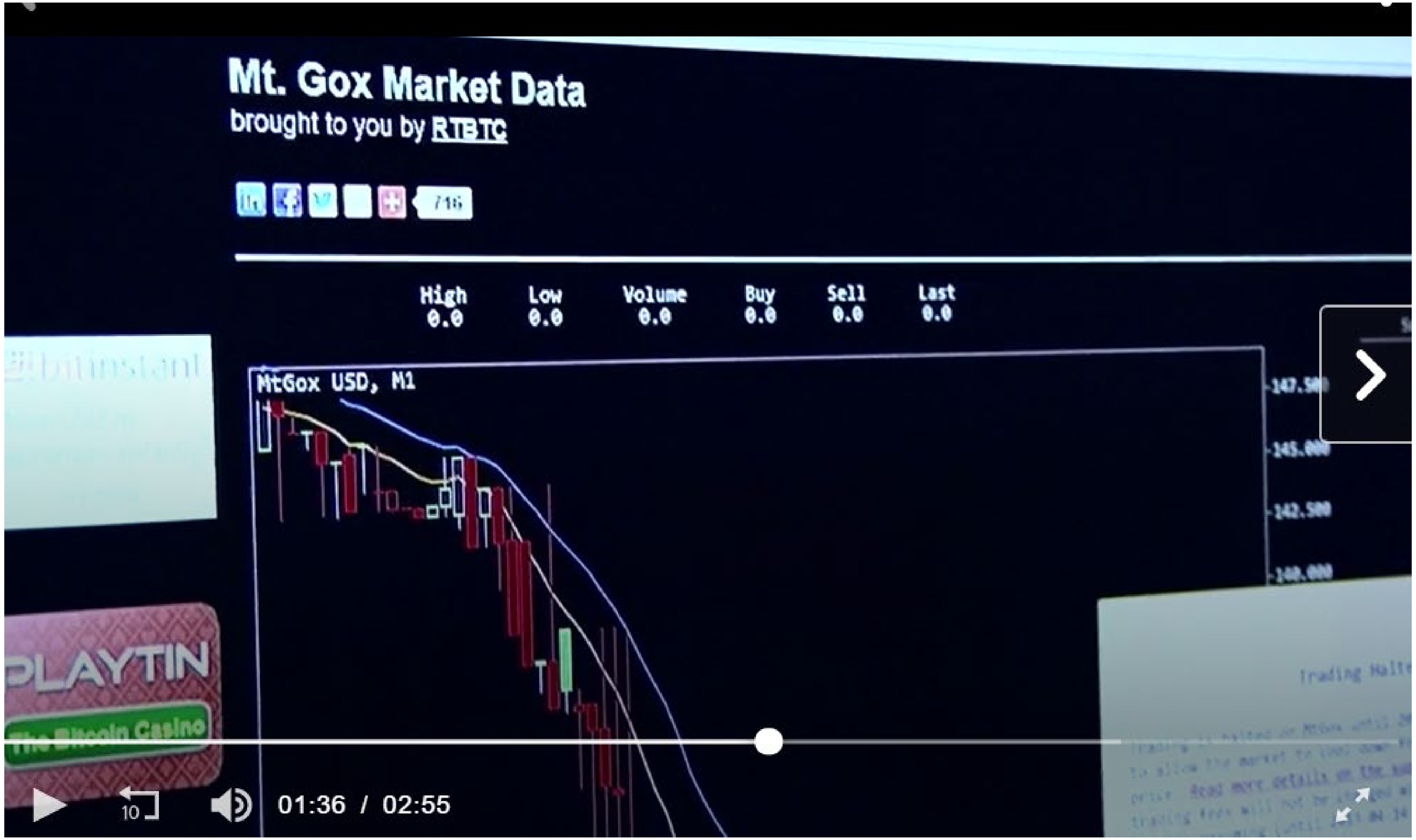
- Blockchain is a decentralized database

- Bitcoin is the first implementation based on blockchain technology

The Value of Bitcoins?

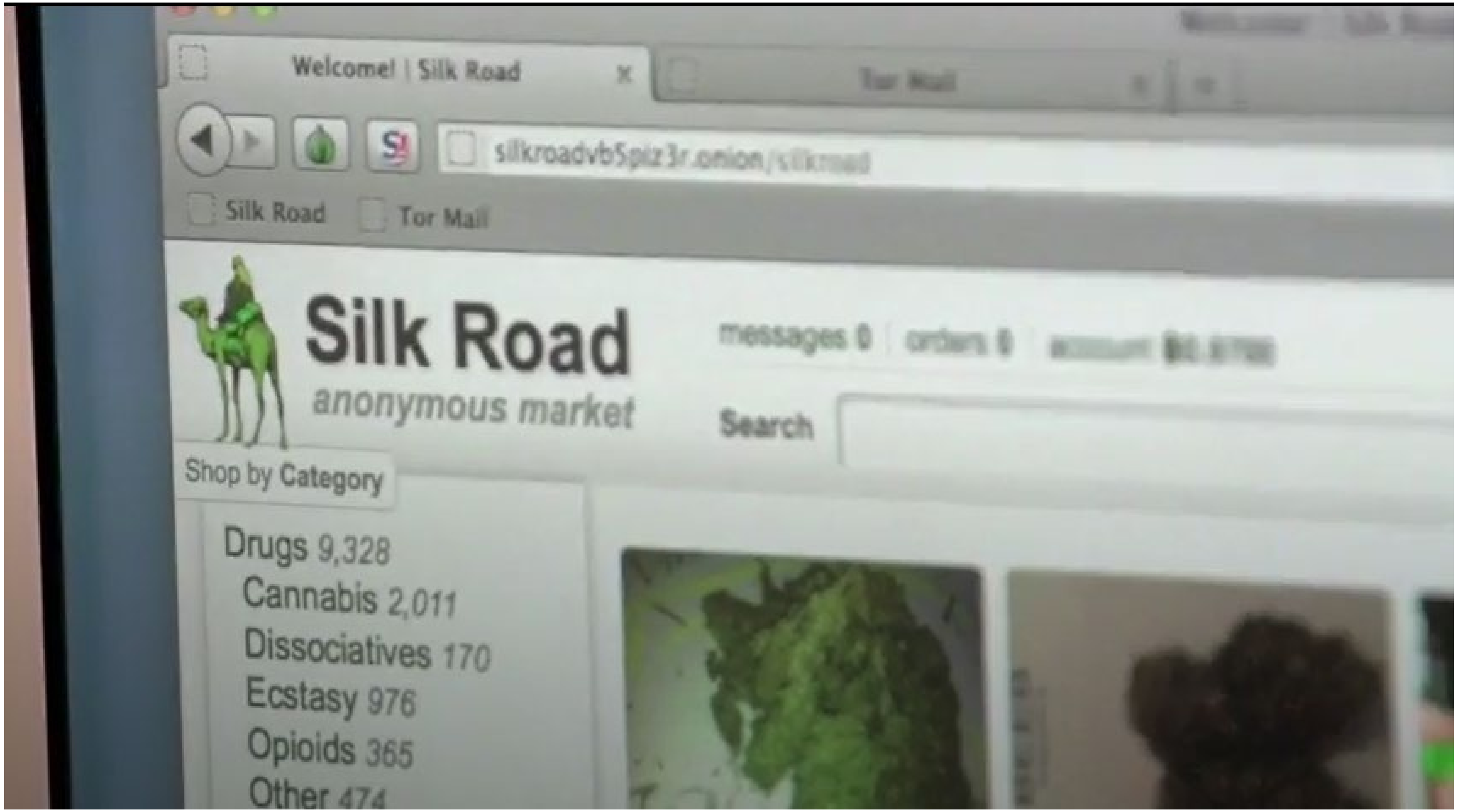
- How should we value Bitcoin?
- Can it replace the fiat money?
- Is it a good investment? How much you would pay to get a bitcoin?
- Why regulations have so different opinions about Bitcoin?
- Be ready for Class Discussion
- Briefly Prepare Two Questions

What is ‘ Mt. Gox’, what happened to it?

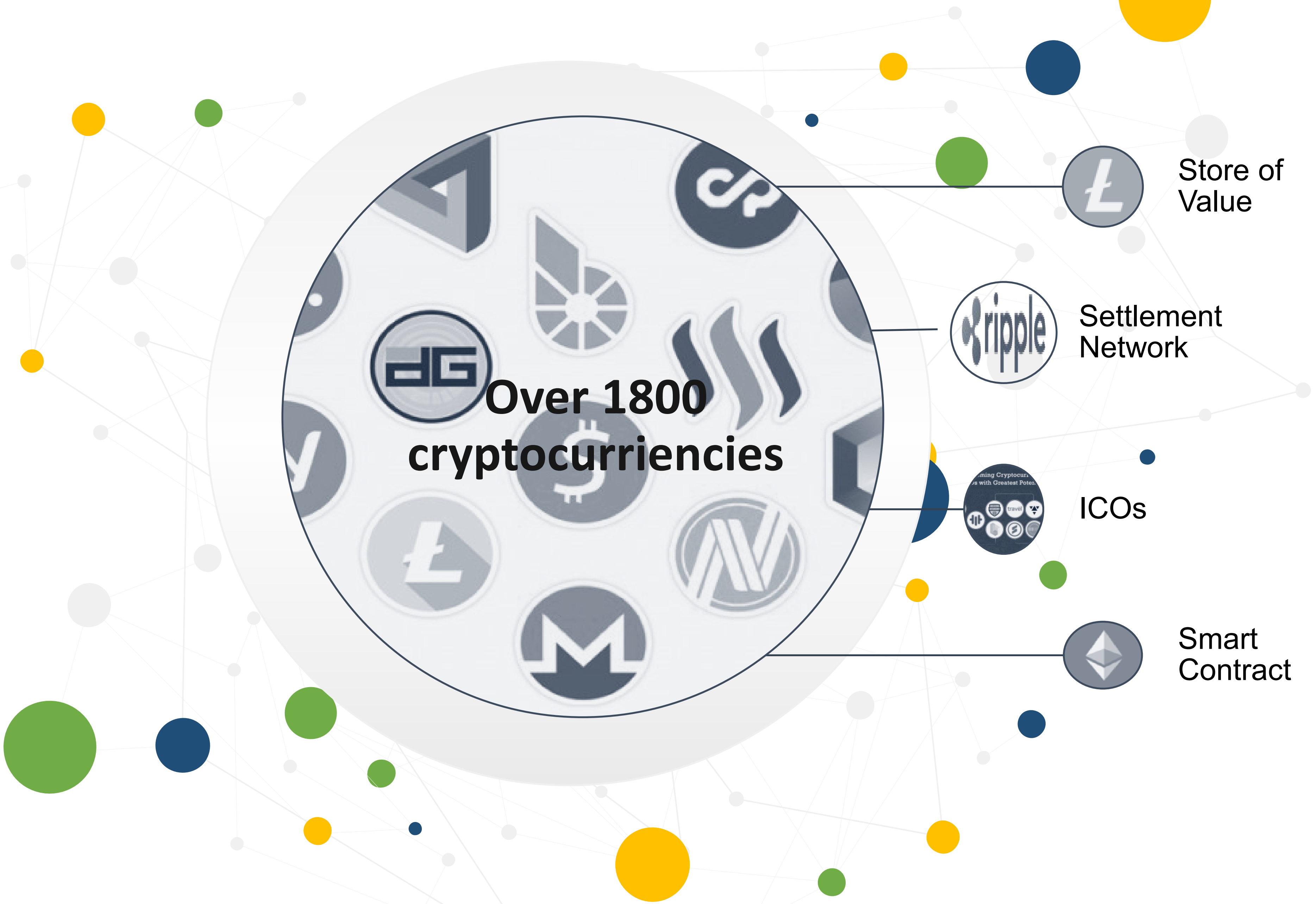


High	Low	Volume	Buy	Sell	Last
0.0	0.0	0.0	0.0	0.0	0.0

What is ‘Silk Road’ ? How ‘Silk Road ‘ relates to Bitcoin?



From Bitcoin to Cryptocurriencies



Over 1800 cryptocurriencies

Store of Value

Settlement Network

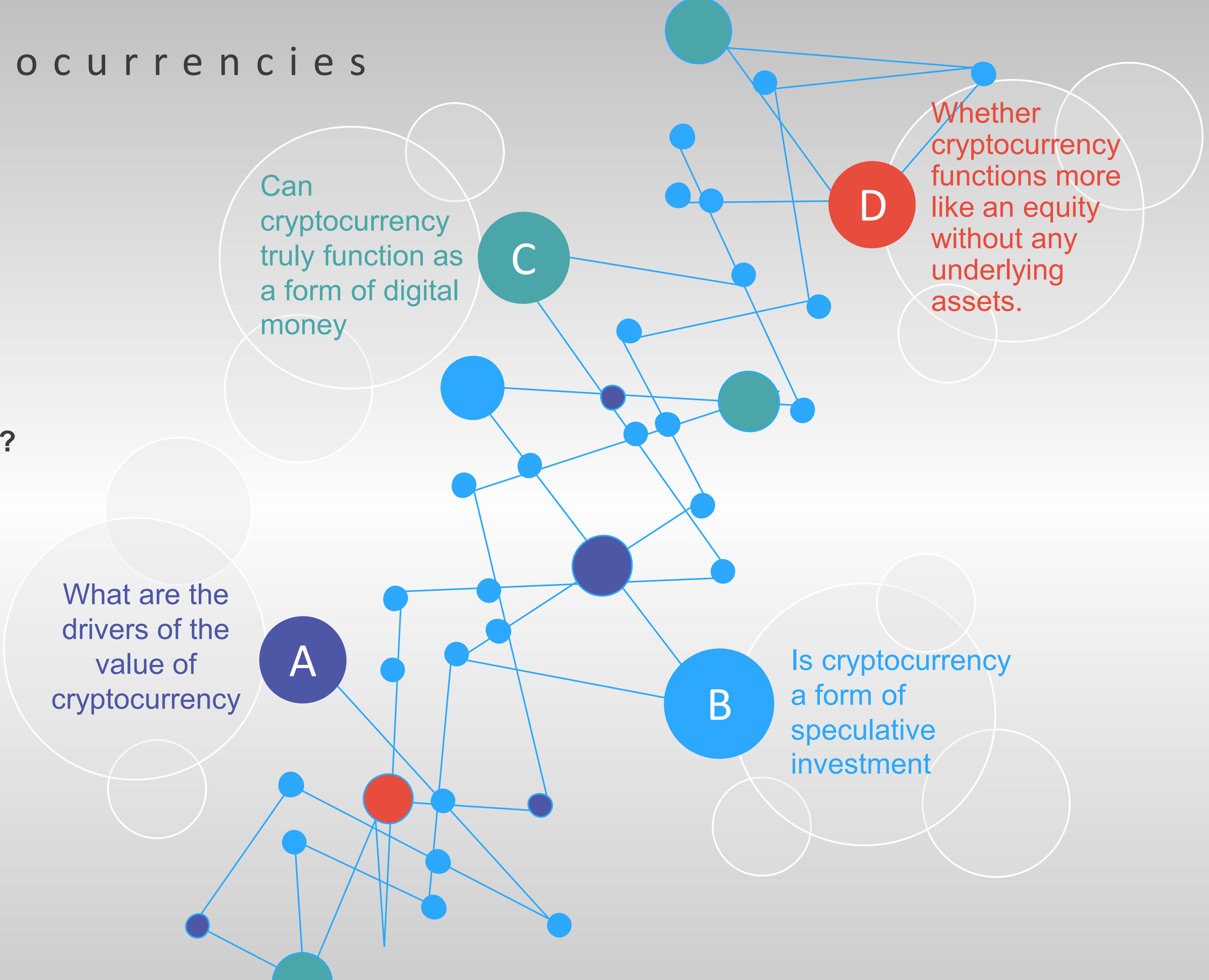
ICOs

Smart Contract

- A centralized intermediary is NOT necessary for MONEY
- Do NOT like centralized banks for philosophical reasons
- Need to hide from government

Evaluate Cryptocurrencies

- A **Value Drivers?**
- B **Speculative Investment?**
- C **Function as Money?**
- D **A Financial Asset?**



Can cryptocurrency truly function as a form of digital money

Whether cryptocurrency functions more like an equity without any underlying assets.

What are the drivers of the value of cryptocurrency

Is cryptocurrency a form of speculative investment

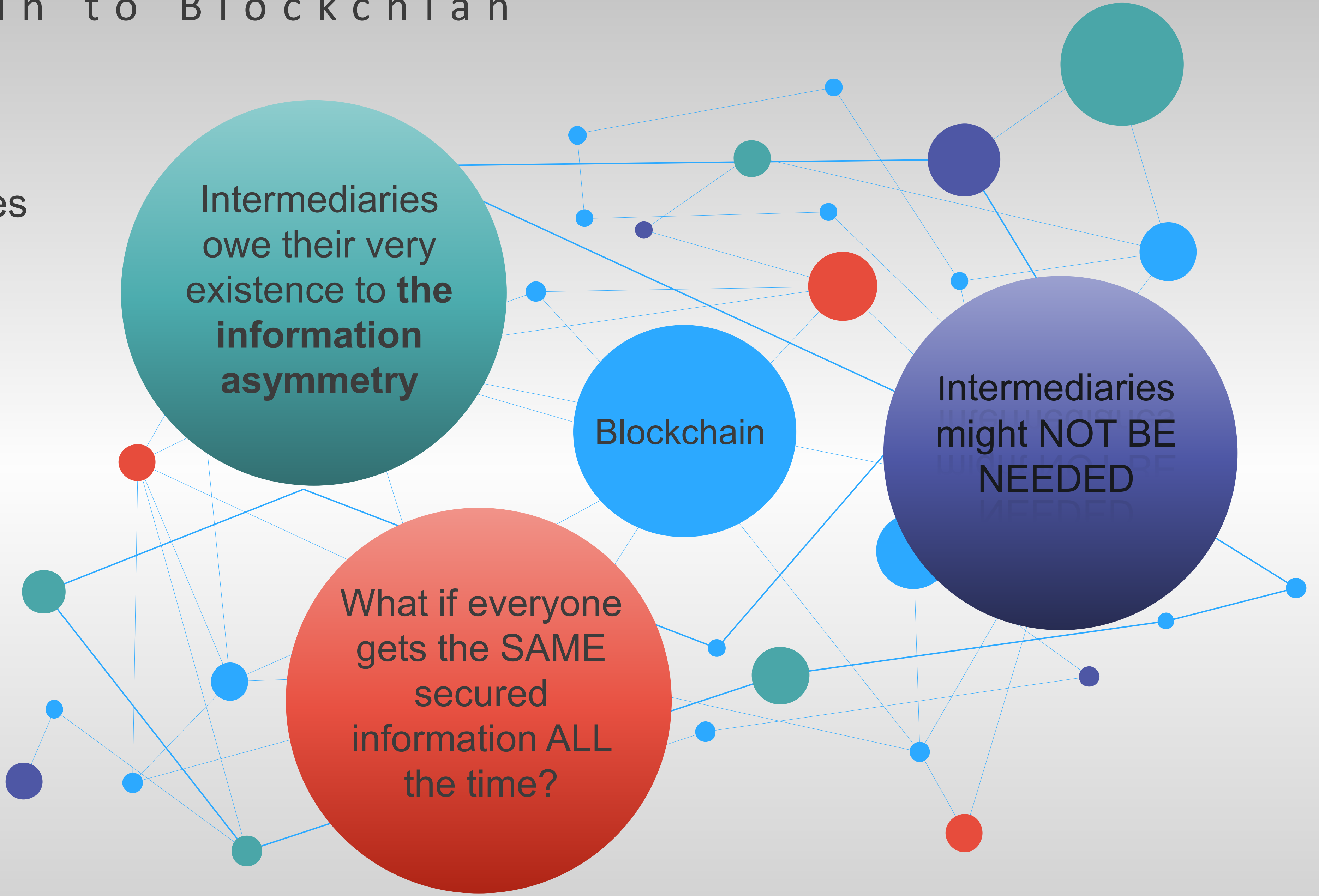
From Bitcoin to Blockchian

Cryptocurrencies

Will remain ‘niche monies’

Blockchain

A Disruptive Technology with grate potential to **reshape** the financial industry



Intermediaries owe their very existence to **the information asymmetry**

Blockchain

What if everyone gets the SAME secured information ALL the time?

Intermediaries might NOT BE NEEDED